



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellants: Oliver et al.
Serial No.: 10/815,512
For: USE OF NODES TO MONITOR OR MANAGE PEER TO PEER
NETWORKS
Filed: 1 APR 2004
Examiner: Kimbrom T. Hailu
Art Unit: 2616
Confirmation No.: 1300
Customer No.: 27,623

Attorney Docket Nos.: 300203615-2
(USPTO Records indicate 300203615-4)
976.8021USU

APPEAL BRIEF FILED UNDER 35 U.S.C. 134

Mail Stop Appeal Brief - Patents
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Appellants are filing this Appeal Brief under 35 U.S.C. 134 and in accordance with the provisions of 37 C.F.R. 41.37(a), and believe that the Appeal Brief complies with the requirements set forth in 37 C.F.R. 41.37(c). The claims on appeal are set forth in an Appendix, below.

On 8 APR 2008, Appellants mailed a Notice of Appeal. Appellants believe that no petition or fee for an extension of time is required to file this Appeal Brief. However, should Appellants be mistaken, please consider this to be a petition for any required extension of time, and please then also charge Deposit Account No. 08-2025 for the required fee. Likewise, the Commissioner is hereby authorized to charge Deposit Account No. 08-2025 for any required fee not submitted herewith, or submitted incorrectly, so as to maintain the pendency of the above-identified patent application.

(i) Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, L.P.

(ii) Related Appeals and Interferences

The undersigned attorney is not aware of any related appeals or interferences.

(iii) Status of the Claims

Claims 1 - 22 are pending in this application, and are the subject of this Appeal.

In an Office Action mailed 8 JAN 2008 (hereinafter "the Office Action"), the Examiner made final his rejection of claims 1 – 22. More specifically, the status of the claims is as follows:

Claim 1: objected to and rejected.

Claims 2 – 22: rejected.

(iv) Status of Amendments

No amendments were proposed subsequent to final rejection.

(v) Summary of Claimed Subject Matter

This Summary makes reference to FIGS. 1, 2, 4 and 9. These figures are provided below, at the end of the Summary.

FIG. 1 is a schematic illustration of a network of computer entities arranged on a peer to peer basis, where each computer is provided with a peer to peer protocol for interacting with other computers in the network. Each of a plurality of computer entities 100-103 communicates with one or more of the other computer entities within the network, and can act either as a client to any other computer entity in the network, and/or as a server to another computer entity. Each computer entity therefore has two modes of operation, firstly acting as a client, where for example it may access data or services stored on another computer entity in a network, or secondly acting as a server, in which case another computer entity may access data or services stored on the computer entity itself. In a general case of a peer to peer environment of connected computer entities, each computer entity represents topologically a node in a network. Connectivity between nodes can be arbitrary in the general case, with any node in the network connecting to any other node in the network.

Within the peer to peer network of FIG. 1, each peer computer contributes resources for use by other computers, as well as consuming services of the network. During periods of inactivity, any spare resources, such as data processing capacity, data storage capacity, connectivity resource or the like, are used to perform a distributed management function. The management functionality is packaged with a peer to peer overlay protocol, and is arranged to activate when the peer to peer protocol is installed or is activated, so that the computer entity is made to operate the management activity when it joins in a peer to peer network. In a specific mode of implementation, operation of the management functionality is activated as a condition of operating the peer to peer protocol.

Monitoring and management may include the following activities:

- Remote virus scanning of other computer entities in the network.
- Observing group behavior in a group of computer entities within the network

- Generating alert messages to alert other computer entities in the network that a particular computer entity is faulty or is misbehaving
- Generating virus alert messages to alert other computer entities in the network that a particular computer entity has a virus
- Placing a faulty computer entity into quarantine
- Performing a diagnosis of one or more faulty computer entities in the network.
- Application of voting protocols for recovering from large network failures.
- Detecting security breaches in said network.
- Detecting performance problems of computers in said network.

FIG. 2 is a schematic illustration of a computer entity that is a peer member of a network of peer to peer computer entities. A computer 200 comprises one or more communications ports 201 for communicating with other computer entities within the network; a data processor 202; a memory device 203; a data storage device 204, for example a hard disk data storage device or a RAID array; a user interface 205, for example comprising a visual display monitor, keyboard and pointing device such as a mouse, trackball, or the like; an operating system 206, for example Microsoft Windows, Linux, or Unix; a peer to peer network protocol layer 207 comprising a middle ware program component for applying a peer to peer network protocol, for example the known Gnutella protocol or similar; a network management application 208, as provided by a specific embodiment; a set of files 209, for example data files, mp3 files, image data files, text data files or the like which may be made available for use by one or more other computers in the network, one or a plurality of local applications 210 for providing local functionality of the computer; and one or more service applications 211 for providing a service, which can be assessed by other computers within the network.

FIG. 4 is a schematic illustration of a computer entity that is enabled to provide network management services within a peer to peer network. The computer entity comprises a set of resources 401, including data processing capability, bit rate capacity (bandwidth), data storage, and data content, for example music files, images files, text files; a resource encapsulation layer 402 which receives service requests from one or more peer computers and/or a user interface of the computer, the encapsulation layer encapsulating the details of supply of resources from the other peer computers or

human users; a set of higher level services 403, which can be accessed by way of service requests received from other peer computer entities within the network, or from a human user of the computer entity, the higher level services comprising for example e-commerce services or the like; and a set of core services 404 including network management services, including network overlay services for establishing the computer as a member of a community of peer to peer connected computers in a peer to peer network, accounting functionality, fault diagnosis functionality and security services. The peer to peer overlay services govern how the peer computer entity communicates with other peer computer entities. Within the core services 404, the network management services and the peer to peer overlay functionality are linked, such that whenever the computer is engaging in a peer to peer network using the peer to peer overlay services, the network management functionality is automatically activated.

FIG. 9 illustrates, schematically, process steps carried out by a peer member for determining a local and global policy towards a specific target member of a peer to peer network. The local peer computer entity may test the target computer entity in process 900 for a particular parameter to be measured, for example, whether the target computer entity is faulty, or is freeloading. Various test procedures can be involved, such as requesting a file or service, or testing a received file for viruses. In process 901, if the target computer entity is tested to have a detrimental characteristic, such as being faulty or freeloading, then in step 902, the local computer generates a local policy towards the target computer entity, in this example the policy being to exclude the target computer entity from the network. The policy may be adopted from a set of nodes pre-stored in the management program to take account of various situations such as freeloading, or a virus. In process 903, the local computer entity broadcasts its local policy data concerning the target computer to all other computer entities in the network of which it is aware, to inform those computer entities of the local computer entity's local policy towards the target computer. In process 904, the local computer entity collects responses from other computers in the network, concerning their local policies towards the target computer. In process 905, the local computer entity applies a voting procedure comprising a set of stored voting rules, in which each of the responses received from the other computer entities in the network, concerning the target computer are considered, and resulting in an overall vote as to whether the target computer entity will be excluded from the network or not. The voting rules are implementation specific, and may be by a simple majority rule, or by a pre-set percentage number of the computer entities voting that the computer target be excluded from the network. In process 906, the local computer entity adopts as its

local policy a policy which has been elected by the voting procedure carried out in process 905. For example, where the majority vote is in favor of retaining the target computer entity on the network, the local computer entity will follow the result of the majority vote, and even though it has tested the target computer entity to be faulty, it will apply the majority vote in order to retain that target computer entity in the local computer entity's own list of members of the peer network.

Concise Explanation of Each of the Independent Claims

The present application contains five independent claims, namely claims 1, 5, 11, 16 and 17. Below, Appellants are providing a concise explanation of the subject matter defined in each of the independent claims. The explanation refers to the specification by page and line number, and to FIGS. 1, 2, 4 and 9 by reference characters.

CLAIM 1. A method (FIG. 4, core services 404; FIG. 9, steps 901 - 906) performed by a first computer entity, said method comprising:

operating a peer to peer protocol (FIG. 1, computer entities 100 - 103; page 5, lines 11 - 14) for enabling said first computer entity (page 16, line 6, "local peer computer entity") to utilise a resource of a second computer entity (page 16, line 6, "target computer entity") in a peer to peer network (page 5, lines 17 - 21), and for enabling said second computer entity to utilise a resource of said first computer entity in said peer to peer network (page 5, lines 17 - 21); and
operating a process (FIG. 9, steps 903 - 906; page 16, line 6 - page 17, line 2), in cooperation with a third computer entity (page 16, line 17, "other computer entities") of said peer to peer network, for managing said second computer entity,
wherein said process is automatically invoked whenever said first computer entity takes part in said peer to peer network using said peer to peer protocol (FIG. 4, core services 404; page 10, lines 29 - 32).

CLAIM 5. A method (FIG. 9, steps 901 - 906) performed by a first computer entity (page 16, line 6, "local peer computer entity") in a peer to peer network, said method comprising:

determining a local policy for management (FIG. 9, step 902; page 16, lines 10 – 15) of a second computer entity (page 16, line 6, “target computer entity”) in said peer to peer network; receiving (FIG. 9, step 904; page 16, lines 19 – 21), from a third computer entity (page 16, line 17, “other computer entities”) in said peer to peer network, a message describing a policy determined by said third computer entity for management of said second computer entity; and determining from said policy determined by said third computer entity, and from said local policy, a network management policy to be applied by said first computer entity to said second computer entity (FIG. 9, steps 905 – 906; page 16, lines 21 – 30).

CLAIM 11. A first computer entity comprising:

a peer to peer networking component (FIG. 2, peer to peer network protocol layer 207; page 7, lines 6 – 8; FIG. 4, items 401 – 403; page 10, lines 10 – 23) for allowing said first computer entity (page 16, line 6, “local peer computer entity”) to engage other computer entities in a peer to peer network on a peer to peer basis; and a network management component (FIG. 2, network management application 208; page 7, lines 8 – 9; FIG. 4, core services 404 including network management services; page 10, lines 23 – 27; FIG. 9, steps 901 – 906; page 16, line 6 – page 17, line 2) for enabling said first computer entity to participate in management of a second computer entity (page 16, line 6, “target computer entity”) in said peer to peer network, in cooperation with a third computer entity (page 16, line 17, “other computer entities”) in said peer to peer network, wherein said network management component is configured to operate automatically, whenever said peer to peer networking component operates to allow said computer entity to take part in said peer to peer network (FIG. 4, core services 404 including network management services; page 10, line 29 – 32).

CLAIM 16. A data storage media comprising:

program data for controlling a first computer entity to perform a method that includes:

operating a peer to peer protocol (page 9, lines 19 – 20, “peer to peer protocol software”) for enabling said first computer entity (page 16, line 6, “local peer computer entity”) to utilise a resource of a second computer entity (page 16, line 6, “target computer

entity”) in a peer to peer network, and for enabling said second computer entity to utilise a resource of said first computer entity in said peer to peer network; and operating a process (page 9, line 20, “network management service program”; FIG. 9, steps 901 – 906; page 16, line 6 – page 17 line 2), in cooperation with a third computer entity (page 16, line 17, “other computer entities”) in said peer to peer network, for managing said second computer entity, wherein said process is automatically invoked (page 9, lines 27 – 29, “automatic operation of the management service program”) whenever said first computer entity takes part in said peer to peer network using said peer to peer protocol.

CLAIM 17. A method performed by a first computer entity (page 16, line 6, “local peer computer entity”), said method comprising:

operating a peer to peer protocol (page 5, lines 9 – 21, “peer to peer protocol”) for enabling said first computer entity to utilise a resource of a second computer entity in a peer to peer network, and for enabling said second computer entity to utilise a resource of said first computer entity in said peer to peer network; and managing (FIG. 9, steps 901 – 906; page 16, line 6 – page 17, line 2) said second computer entity (page 16, line 6, “target computer entity”), in cooperation with a third computer entity (page 16, line 17, “other computer entities”) in said peer to peer network.

Title: Use of Nodes to Monitor/Manage Peer to Peer Networks
Inventors: Huw Edward Oliver, Simon Crouch, Hans Daanen
Ref: 300203615

1/9

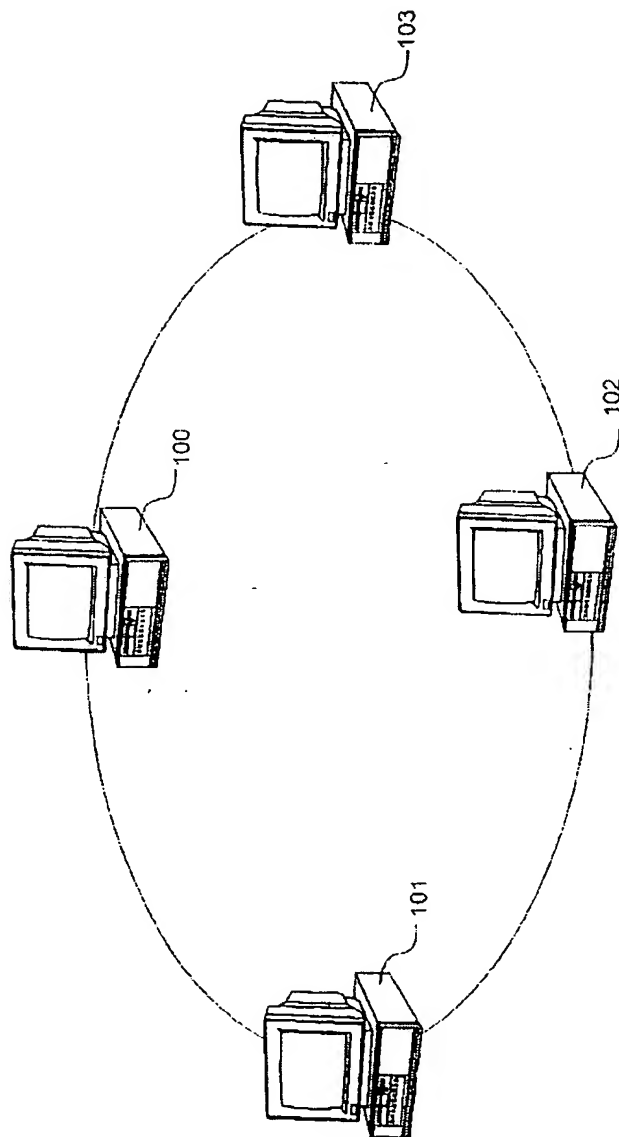


Fig.1

Title: Use of Nodes to Monitor/Manage Peer to Peer Networks
Inventors: Huw Edward Oliver, Simon Crouch, Hans Daanen
Ref: 300203615

2/9

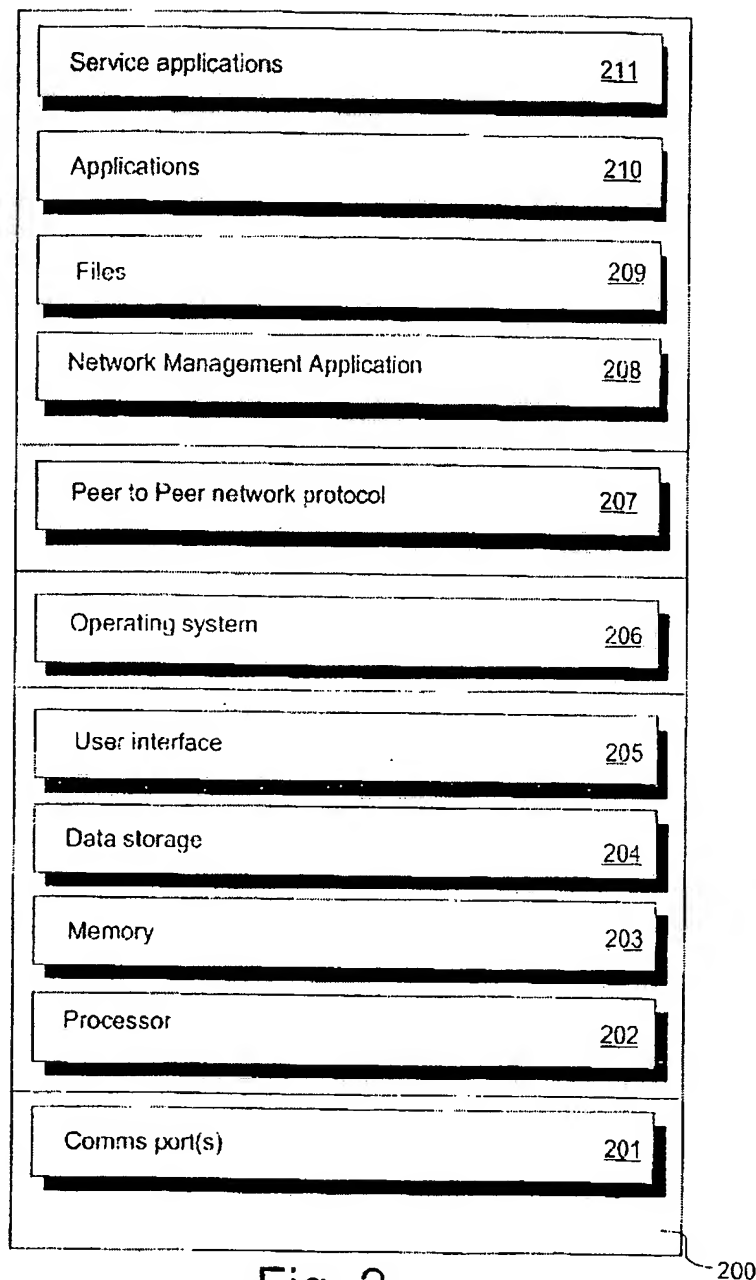


Fig. 2

Title: Use of Nodes to Monitor/Manage Peer to Peer Networks
Inventors: Huw Edward Oliver, Simon Crouch, Huns Daanen
Ref: 300203615

4/9

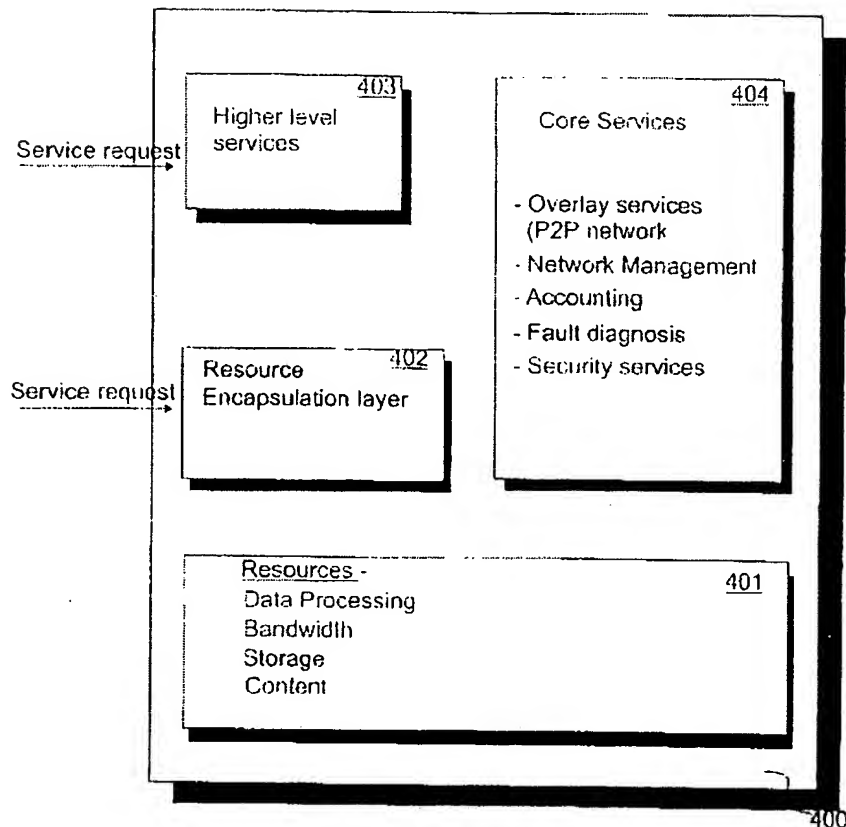


Fig. 4

Title: Use of Nodes to Monitor/Manage Peer to Peer Networks
Inventors: Huw Edward Oliver, Simon Crouch, Hans Daanen
Ref: 300203615

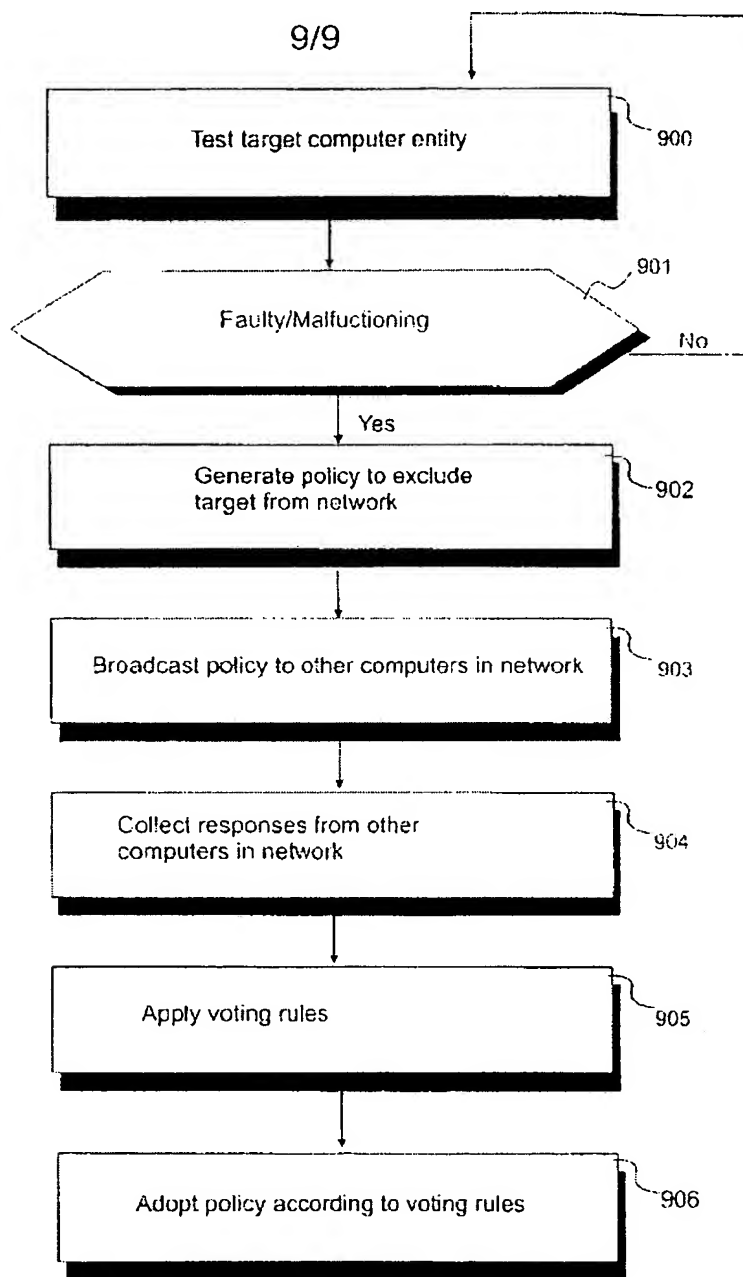


Fig. 9

(vi) Grounds of Rejection to be Reviewed on Appeal

The first issue presented for review is the propriety of the Examiner's final rejection of claim 16 under 35 U.S.C. 101 as being directed to non-statutory subject matter.

The second issue presented for review is the propriety of the Examiner's final rejection of claims 1, 5, 11, 16 and 17 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

The third issue presented for review is the propriety of the Examiner's final rejection of claims 1 – 3, 5 – 7 and 10 – 22 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 7,127,613 to Pabla et al. (hereinafter "the Pabla et al. patent").

The fourth issue presented for review is the propriety of the Examiner's final rejection of claim 9 under 35 U.S.C. 103(a) as being unpatentable over the Pabla et al. patent in view of U.S. Patent No. 7,137,145 to Gleichauf (hereinafter "the Gleichauf patent").

The fifth issue presented for review is the propriety of the Examiner's final rejection of claims 4 and 8 under 35 U.S.C. 103(a) as being unpatentable over the Pabla et al. patent in view of the Gleichauf patent, in further view of a document by Golle (hereinafter "the Golle document").

(vii) Argument

(1) The first issue presented for review is the propriety of the Examiner's final rejection of claim 16 under 35 U.S.C. 101 as being directed to non-statutory subject matter.

Claim 16 provides for a data storage media comprising program data for controlling a first computer entity to perform a method that includes, *inter alia*,

operating a peer to peer protocol for enabling said first computer entity to utilise a resource of a second computer entity in a peer to peer network, and for enabling said second computer entity to utilise a resource of said first computer entity in said peer to peer network; and

operating a process, in cooperation with a third computer entity in said peer to peer network, for managing said second computer entity.

The Office Action, section 3, contends that claim 16 is not statutory on the grounds that “a data storage media comprising: program data for controlling a first computer entity” is not tangible, since the claim doesn’t require any physical transformation and/or is not being executed by a computer. The Office Action further contends that the program data or instructions that are stored in the media have to be executed such as by a processor, and therefore, the invention as claimed does not produce a useful, concrete and tangible result. Appellants respectfully disagree.

“Functional descriptive material” consists of data structures and computer programs that impart functionality when employed as a computer component. When functional descriptive material is recorded on some computer readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized (MPEP 2106.01).

A computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program’s functionality to be realized, and is thus statutory. (MPEP 2106.01, citing *In re Lowry*, 32 F.3d at 1583-84, 32 USPQ2d at 1035).

Appellants submit that whereas claim 16 recites **a data storage media** comprising **program** data for **controlling a first computer entity to perform a method** that includes, *inter alia*, operating a peer to peer protocol, and operating a process, it recites a computer-readable medium encoded with a computer program that is a computer element that defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program’s functionality to be realized, and is thus statutory. Accordingly, Appellants submit that claim 16 fulfills the requirements of 35 U.S.C. 101.

Appellants believe that the Office Action’s contention that the invention as claimed does not produce a useful, concrete and tangible result, is misplaced. Appellants believe that the criteria of a

useful, concrete and tangible result are for an evaluation of whether the claimed invention is a practical application of an abstract idea, a law of nature, or a natural phenomenon, which only arises in a case where the Examiner has first determined that the claimed invention is an abstract idea, a law of nature, or a natural phenomenon. In the present case, the Examiner has not asserted that the claim 16 is claiming an abstract idea, a law of nature, or a natural phenomenon, and therefore, Appellants believe that the useful, concrete and tangible result test is misplaced.

Nevertheless, even if claim 16 is evaluated under the useful, concrete and tangible result test, Appellants submit that operating a process, in cooperation with a third computer entity in said peer to peer network, for **managing said second computer entity**, is a useful, concrete and tangible result, i.e., the management of the second computer entity. Thus, even under the test being applied in the Office Action, claim 16 fulfills the requirements of 35 U.S.C. 101.

Appellants are requesting reconsideration and a withdrawal of the section 101 rejection of claim 16.

(2) The second issue presented for review is the propriety of the Examiner's final rejection of claims 1, 5, 11, 16 and 17 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

(a) Claims 1 and 16 stand or fall together.

Claim 1 provides for a method performed by a first computer entity. The method includes, *inter alia*,

operating a peer to peer protocol for enabling said first computer entity to utilise a resource of a second computer entity in a peer to peer network, and for enabling said second computer entity to utilise a resource of said first computer entity in aid peer to peer network; and operating a process, in cooperation with a third computer entity of said peer to peer network, for managing said second computer entity.

The Office Action, section 7, contends that “operating a process, in cooperation with a third computer entity of said peer to peer network, for managing said second computer entity”, is not found in the specification, and that the specification does not even mention a third computer entity.

FIG. 9 illustrates, schematically, process steps carried out by a peer member for determining a local and global policy towards a specific target member of a peer to peer network. The process involves a local peer computer entity (page 16, line 6), a target computer entity (page 16, line 6), and other computer entities (page 16, line 16), and more specifically, the local computer entity operating a process in cooperation with the other computer entities, for managing the target computer entity (FIG. 9, steps 903 – 906). In the context of claim 1, the local computer entity is the **first computer entity**, the target computer is the **second computer entity**, and the other computer entities include the **third computer entity**. Thus, Appellants submit that claim 1 complies with the written description.

Claim 16 includes recitals similar to those of claim 1. Accordingly, Appellants submit that claim 16 also complies with the written description.

Reconsideration and a withdrawal of the section 112 rejection of claims 1 and 16 are respectfully requested.

(b) Claim 5 stands alone.

Claim 5 provides for a method performed by a first computer entity in a peer to peer network. The method includes:

- determining a local policy for management of a second computer entity in said peer to peer network;
- receiving, from a third computer entity in said peer to peer network, a message describing a policy determined by said third computer entity for management of said second computer entity; and
- determining from said policy determined by said third computer entity, and from said local policy, a network management policy to be applied by said first computer entity to said second computer entity.

The Office Action, section 7, contends that “from a third computer entity in said peer to peer network, a message describing policy determined by said [third] computer entity for management of said second computer entity; and determining from said policy determined by said third computer entity” is not disclosed.

FIG. 9 illustrates, schematically, process steps carried out by a peer member for determining a local and global policy towards a specific target member of a peer to peer network. The process involves a local peer computer entity (page 16, line 6), a target computer entity (page 16, line 6), and other computer entities (page 16, line 16). Step 904 (page 16, lines 19 – 21) involves, receiving, from a third computer entity (i.e., a member of the other computer entities) in said peer to peer network, a message describing a policy determined by said third computer entity for management of said second computer entity (i.e., the target computer). Steps 905 – 906 (page 16, lines 21 – 30) involve determining from said policy determined by said third computer entity, and from said local policy, a network management policy to be applied by said first computer entity to said second computer entity. In the context of claim 5, the local computer entity is the **first computer entity**, the target computer is the **second computer entity**, and the other computer entities include the **third computer entity**. Thus, Appellants submit that claim 5 complies with the written description.

Reconsideration and a withdrawal of the section 112 rejection of claim 5 are respectfully requested.

(c) Claims 11 and 17 stand or fall together.

Claim 11 provides for a first computer entity that includes, *inter alia*,
a peer to peer networking component for allowing said first computer entity to engage other
computer entities in a peer to peer network on a peer to peer basis; and
a network management component for enabling said first computer entity to participate in
management of a second computer entity in said peer to peer network, in cooperation with a
third computer entity in said peer to peer network,

The Office Action, section 7, contends that “managing or participate in management of a second computer entity in said peer to peer network, in cooperation with a third computer entity in said peer to peer network” is not found in the specification, and that the specification does not even mention a third computer entity.

The specification, with reference to FIG. 2, mentions a network management application 208 (page 7, lines 8 – 9), and with reference to FIG. 4, a core services 404 that includes network management services (page 10, lines 23 – 27). FIG. 9 illustrates, schematically, process steps carried out by a peer member for determining a local and global policy towards a specific target member of a peer to peer network. The process involves a local peer computer entity (page 16, line 6), a target computer entity (page 16, line 6), and other computer entities (page 16, line 16), and more specifically, a network management component (e.g., network management application 208) for enabling the local peer computer entity to participate in management of the target computer entity in said peer to peer network, in cooperation with other computer entities in the peer to peer network (FIG. 9, steps 901 – 906; page 16, line 6 – page 17, line 2). In the context of claim 11, the local computer entity is the **first computer entity**, the target computer is the **second computer entity**, and the other computer entities include the **third computer entity**. Thus, Appellants submit that claim 11 complies with the written description.

Claim 17 includes recitals similar to those of claim 11. Accordingly, Appellants submit that claim 17 also complies with the written description.

Reconsideration and a withdrawal of the section 112 rejection of claims 11 and 17 are respectfully requested.

(3) The third issue presented for review is the propriety of the Examiner’s final rejection of claims 1 – 3, 5 – 7 and 10 – 22 under 35 U.S.C. 102(e) as being anticipated by the Pabla et al. patent.

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

In order to anticipate a claim under Section 102 and render it unpatentable, a single prior art reference must not only expressly or inherently disclose each and every element set forth in the claim, but the reference must also be enabling, i.e. it must clearly put the claimed subject matter in the possession of the public. *In re Brown*, 329 F. 2d 1066, 144 USPQ 245 (CCPA 1964); *In re Kalm*, 378 F. 2d 959, 1154 USPQ 10 (CCPA 1967); *Rem-Cru Titanium, Inc. v. Watson*, 147 F. Supp. 915 112 USPQ 88 (Dist. Ct., DC 1956); *Akzo N.V. v. United States ITC*, 808 F 2d 1471, 1 USPQ 2d 1241 (Fed. Cir. 1986); and *In re Spada*, 911 F 2d 705, 15 USPQ 2d 1655 (Fed. Cir. 1990). The mere disclosure of concepts does not anticipate.

(a) Claims 1 – 3, 16, 18 and 21 stand or fall together.

Claim 1 provides for a method performed by a first computer entity. The method includes, *inter alia*, (a) operating a peer to peer protocol for enabling the first computer entity to utilise a resource of a second computer entity, and for enabling the second computer entity to utilise a resource of the first computer entity, and (b) operating a process, in cooperation with a third computer entity, for managing the second computer entity.

The Office Action, near the top of page 7, suggests that several passages in the Pabla et al. patent are descriptive of operating a process, in cooperation with a third computer entity, for managing the second computer entity. Table 1, below, briefly summarizes the substance of each of the several passages.

TABLE 1

Pabla et al. (citation)	Summary of substance of cited passage
col 12, lines 60 - 62	Mechanisms with which peers may find each other, cooperate with each other, and communicate with each other.
col. 13, lines 51 - 53	Peers may cooperate and communicate with each other by following a set of rules and conventions

Pabla et al. (citation)	Summary of substance of cited passage
col. 18, lines 17 – 39 and 43 - 50	Concerns joining a peer group, voting, finding a peer, and searching for peers
col. 19, lines 32 - 39	Sharing resources
col. 22, lines 17 – 21	Peer group service
col. 1, lines 32 - 34	Client/server relationships

None of the above-noted passages of the Pabla et al. patent discloses an activity that involves two computes cooperating with one another to manage another computer. Thus, the Pabla et al does not disclose a method that includes **a first computer entity** operating a process, **in cooperation with a third computer entity**, for **managing a second computer entity**, as recited in claim 1.

NOTE: The Office Action, in a paragraph that bridges pages 3 and 4, mentions col. 18, line 28, and suggests that the Pabla et al. patent describes computers participating in a vote. The Pabla et al. patent, at col. 18, lines 22 – 30, states:

In one embodiment, peers wishing to join a peer group may first locate a current member of the peer group, and then request to join the peer group. The application to join may either be rejected or accepted by one or more of the current members. In one embodiment, membership acceptance policies may enforce a vote, or alternatively may elect one or more designated group representatives to accept or reject new membership applications. (Emphasis added)

The Office Action, on page 4, states that the Examiner believes that “the members are the peers, which in this case are the computer devices (see fig. 1B, “peer devices”).” Appellants agree that the members are the peers, but disagree with the Examiner’s belief that the peers are the computer devices. The Pabla et al. patent explains that peers are computer users (col. 1, lines 36 – 37). Thus, the above-noted passage is describing a vote being cast by computer users, e.g., humans. Accordingly, Appellants submit that although the Pabla et al. patent mentions a vote, the Pabla et al. patent does not describe a computer device casting a vote to manage another computer.

For the reasons provided above, Appellants submit that the Pabla et al. patent does not anticipate claim 1.

Claims 2, 3 and 18 depend from claim 1. By virtue of this dependence, claims 2, 3 and 18 are also novel over the Pabla et al. patent.

Claim 16 includes recitals similar to those of claim 1. As such, claim 16, is also novel over the Pabla et al. patent.

Claim 21 depends from claim 16. By virtue of this dependence, claim 21 is also novel over the Pabla et al. patent.

Appellants respectfully request reconsideration and a withdrawal of the section 102(e) rejection of claims 1 – 3, 16, 18 and 21.

(b) Claims 5 – 7 and 19 stand or fall together.

Claim 5 provides for a method performed by a first computer entity of a peer to peer network. The method includes, *inter alia*, (a) determining a local policy for management of a second computer entity, (b) receiving, from a third computer entity, a message describing a policy determined by the third computer entity for management of the second computer entity, and (c) determining from the policy determined by the third computer entity, and from the local policy, a network management policy to be applied by the first computer entity to the second computer entity.

The Office Action, in a paragraph that bridges page 7 to page 8, suggests that several passages in the Pabla et al. patent are descriptive of (b) receiving, from a third computer entity, a message describing a policy determined by the third computer entity for management of the second computer entity, and (c) determining from the policy determined by the third computer entity, and from the local policy, a network management policy to be applied by the first computer entity to the second computer entity. Table 2, below, briefly summarizes the substance of each of the passages.

TABLE 2

Pabla et al. (citation)	Summary of substance of cited passage
col. 17, lines 23 – 39	A broadcast message sent to all listening endpoint simultaneously.
col. 18, lines 55 – 59	A content sharing policy.
col. 13, lines 6 – 12	A message that contains a session key.
col. 17, lines 23 – 34	A broadcast message sent to all listening endpoint simultaneously.
col. 21, lines 13 – 16	A content management service to facilitate sharing of content.
col. 24, lines 15 – 23	Peer group advertisements, and a policy to vote for new member approval.
col. 18, lines 55 - 59	A content sharing policy

None of the above-noted passages of the Pabla et al. patent discloses either of a policy determined by a computer for management of another computer, or a use of such a policy in a determination of a network management policy. Consequently, the Pabla et al. patent does not disclose (b) receiving, from a third computer entity, a message describing **a policy determined by the third computer entity for management of the second computer entity**, and (c) **determining from the policy determined by the third computer entity, and from the local policy, a network management policy** to be applied by the first computer entity to the second computer entity, as recited in claim 5.

NOTE: As explained above, during the discussion of claim 1, although the Pabla et al. patent mentions a vote, the Pabla et al. patent does not describe a computer device casting a vote to manage another computer.

For the reasons provided above, Appellants submit that the Pabla et al. patent does not anticipate claim 5.

Claims 6, 7 and 19 depend from claim 5. By virtue of this dependence, claims 6, 7 and 19 are also novel over the Pabla et al. patent.

Appellants are requesting reconsideration and a withdrawal of the section 102(e) rejection of claims 5 – 7 and 19.

(c) Claim 10 stands alone.

Claim 10 depends from claim 5, and further recites, *inter alia*, that determining the network management policy comprises applying a voting protocol in which the first and third computer entities vote.

The Office Action, on page 8, suggests that the Pabla et al. patent, in a passage at col. 18, lines 17 – 32, discloses the substance of claim 10. However, as explained above, during the discussion of claim 1, although the Pabla et al. patent mentions a vote, the vote is being cast by users of a computer, i.e., humans. Therefore, the Pabla et al. patent does not disclose applying a voting protocol in which the first and third **computer entities vote**, as recited in claim 10. Accordingly, Appellants submit that claim 10, by virtue of its dependence on claim 5, and also on its own merits, is novel over the Pabla et al. patent.

Appellants are requesting reconsideration and a withdrawal of the section 102(e) rejection of claim 10.

(d) Claims 11 – 15 and 20 stand or fall together.

Claim 11 provides for a first computer entity that includes, *inter alia*, a network management component for enabling the first computer entity to participate in management of a second computer entity in a peer to peer network, in cooperation with a third computer entity in the peer to peer network.

The Office Action, near the bottom of page 8, suggest that the Pabla et al. patent, in a passage at col. 20, lines 58 – 63, describes the network management component of claim 11. The Pabla et al. patent, at col. 20, lines 58 – 63 states:

High-level services 220 may include such services as the content management services 222 and the search and index system services 224 of this illustration. The core services 210 and high-level services 220 interface through a peer group sharing API 216 to the peer group sharing software 212. The peer group sharing software 212 on the two peers 200 may interface to each other using the low-level peer group sharing protocol 218. High-level services 220 may interface using higher-level protocols. For example, the content management services 222 on the two peers may interface using peer group content

management protocols 226, and the search and index system services 224 may interface using content search and indexing protocols 228.

Although the above-noted passage mentions a variety of services, none of the services involves two computers cooperating with one another to manage another computer. Thus, Appellants submit that the Pabla et al. patent does not describe a network management component for **enabling the first computer entity to participate in management of a second computer entity** in a peer to peer network, **in cooperation with a third computer entity** in the peer to peer network, as recited in claim 11. Accordingly Appellants further submit that the Pabla et al. patent does not anticipate claim 11.

Claims 12 – 15 and 20 depend from claim 11. By virtue of this dependence, claims 12 – 15 and 20 are also novel over the Pabla et al. patent.

Appellants are requesting reconsideration and a withdrawal of the section 102(e) rejection of claims 11 – 15 and 20.

(e) Claims 17 and 22 stand or fall together.

Claim 17 provides for a method performed by a first computer entity. The method includes, *inter alia*, managing a second computer entity, in cooperation with a third computer entity.

The Office Action, on page 10, suggests that the Pabla et al. patent, in passages at col. 20, lines 58 – 63, and col. 21, lines 13 – 16, describes the above-noted feature of claim 17.

Regarding the passage at col. 20, lines 58 – 63, Appellants explained above, during the discussion of claim 11, that although the passage mentions a variety of services, none of the services involves two computers cooperating with one another to manage another computer.

Regarding the passage at col. 21, lines 13 – 16, Appellants noted above, in Table 2, that the passage involves a content management service to facilitate sharing of content. The content management service does not involve two computers cooperating with one another to manage another computer.

Whereas neither of the two above-noted passages involves two computers cooperating with one another to manage another computer, Appellants submit that the Pabla et al. patent does not describe **managing a second computer entity, in cooperation with a third computer entity**, as recited in claim 17. Hence, Appellants further submit that the Pabla et al. patent does not anticipate claim 17.

Claim 22 depends from claim 17. By virtue of this dependence, claim 22 is also novel over the Pabla et al. patent.

Appellants are requesting reconsideration and a withdrawal of the section 102(e) rejection of claims 17 and 22.

(4) The fourth issue presented for review is the propriety of the Examiner's final rejection of claim 9 under 35 U.S.C. 103(a) as being unpatentable over the Pabla et al. patent in view of the Gleichauf patent.

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Furthermore, if an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

Claim 9 depends from claim 5. Above, Appellants explained that the Pabla et al. patent does not anticipate claim 5. Appellants submit that the Gleichauf patent does not make up for the deficiency of the Pabla et al. patent, with respect to claim 5. Accordingly, Appellants further submit that claim 5, and claim 9 by virtue of its dependence on claim 5, are both patentable over the cited combination of the Pabla et al. and Gleichauf patents. Reconsideration and withdrawal of the section 103(a) rejection of claim 9 are respectfully solicited.

(5) The fifth issue presented for review is the propriety of the Examiner's final rejection of claims 4 and 8 under 35 U.S.C. 103(a) as being unpatentable over the Pabla et al. patent in view of the Gleichauf patent, in further view of the Golle document.

Claim 4 depends from claim 1, and claim 8 depends from claim 5. Appellants respectfully submit that the cited combination of the Pabla et al. patent, the Gleichauf patent, and the Golle document does not disclose or suggest either of (a) a method that includes a first computer entity operating a process, in cooperation with a third computer entity, for managing a second computer entity, as recited in claim 1, or (b) a method that includes a first computer entity determining from a policy determined by a third computer entity, and from a local policy, a network management policy to be applied to a second computer entity by the first computer entity, as recited in claim 5. Accordingly, Appellants submit that claims 1 and 5, and claims 4 and 8, by virtue of their respective dependencies, are all patentable over the cited combination of the Pabla et al. patent, the Gleichauf patent, and the Golle document. Reconsideration and withdrawal of the section 103(a) rejection of claims 4 and 8 are respectfully requested.

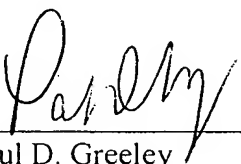
In view of the foregoing arguments, Appellant respectfully requests that the Board of Appeals reverse the final rejection of claims 1 - 22, thereby enabling all of the pending claims to be allowed.

Appellants note that the Office Action, section 2, is rejecting claim 1 because of an informality, and that section 5 is provisionally rejecting several claims. Appellants will address the informality and the provisional rejection after the Office renders a decision regarding the present appeal.

Respectfully submitted,

6/6/08

Date



Paul D. Greeley
Reg. No. 31,019
Attorney for the Appellants
Ohlandt, Greeley, Ruggiero & Perle, L.L.P.
One Landmark Square, 10th Floor
Stamford, CT 06901-2682
Tel: 203-327-4500
Fax: 203-327-6401

(viii) Claims Appendix

The claims on appeal are set forth below.

1. (previously presented) A method performed by a first computer entity, said method comprising:
operating a peer to peer protocol for enabling said first computer entity to utilise a resource of a second computer entity in a peer to peer network, and for enabling said second computer entity to utilise a resource of said first computer entity in said peer to peer network; and operating a process, in cooperation with a third computer entity of said peer to peer network, for managing said second computer entity, wherein said process is automatically invoked whenever said first computer entity takes part in said peer to peer network using said peer to peer protocol.
2. (previously presented) The method as claimed in claim 1, wherein said process comprises: determining a policy by which said first computer entity will interact with said second computer entity.
3. (previously presented) The method as claimed in claim 1, wherein said process comprises: adopting a policy towards said second computer entity, wherein said policy is selected from a set of pre-determined policies for determining a relationship between said first computer entity and said second computer entity.
4. (previously presented) The method as claimed in claim 1, wherein managing said second computer entity comprises a process selected from the group consisting of:
placing said second computer entity in quarantine;
controlling access by said second computer entity to a communal resource stored on said first computer entity; and
applying a charge for utilisation by said second computer entity of a communal resource.

5. (previously presented) A method performed by a first computer entity in a peer to peer network, said method comprising:

determining a local policy for management of a second computer entity in said peer to peer network;
receiving, from a third computer entity in said peer to peer network, a message describing a policy determined by said third computer entity for management of said second computer entity; and
determining from said policy determined by said third computer entity, and from said local policy, a network management policy to be applied by said first computer entity to said second computer entity.

6. (previously presented) The method as claimed in claim 5, further comprising:
broadcasting said network management policy to a plurality of peer computers within said peer to peer network.


7. (previously presented) The method as claimed in claim 5, comprising:
monitoring said second computer entity; and
depending upon a result of said monitoring, adopting a pre-determined policy from a stored set of policies, and applying said pre-determined policy to said second computer entity.

8. (previously presented) The method as claimed in claim 5, wherein a said network management policy comprises a policy selected from the group consisting of:

a policy for determining whether or not to place said second computer entity into quarantine;
a policy for generating a virus alert message for alerting other computer entities in the peer to peer network that a said second computer entity has a virus;
a policy for generating a fault alert message for alerting other computer entities in the peer to peer network that said second computer entity is faulty;
a policy determining whether to exclude said second computer entity from accessing a particular type of resource;
a policy for determining whether to exclude said second computer entity from the peer to peer network;

a policy for control of access by said second computer entity to a communal resource; and
a charging policy for charging said second computer entity for accessing a resource.

9. (previously presented) The method as claimed in claim 5, comprising applying a monitoring operation to said second computer entity, wherein said monitoring operation is selected from the group consisting of:

- 
- a monitoring operation for remote virus scanning of said second computer;
 - a monitoring operation for observing a group behavior of a group of target computer entities within said peer to peer network;
 - a monitoring operation for detecting a security breach in said peer to peer network;
 - a monitoring operation for detecting a performance problem of said second computer.

10. (previously presented) The method as claimed in claim 5, wherein said determining said network management policy comprises:

- applying a voting protocol in which said first and third computer entities vote, and thereby adopt a common policy for said network management policy.

11. (previously presented) A first computer entity comprising:

- a peer to peer networking component for allowing said first computer entity to engage other computer entities in a peer to peer network on a peer to peer basis; and
 - a network management component for enabling said first computer entity to participate in management of a second computer entity in said peer to peer network, in cooperation with a third computer entity in said peer to peer network,
- wherein said network management component is configured to operate automatically, whenever said peer to peer networking component operates to allow said computer entity to take part in said peer to peer network.

12. (previously presented) The first computer entity as claimed in claim 11, wherein said network management component is activated whenever said peer to peer networking component is operational.

13. (previously presented) The first computer entity as claimed in claim 11, wherein said network management component comprises program data that controls resources of said peer to peer network to perform a network management service.

14. (previously presented) The first computer entity as claimed in claim 11, wherein said network management component applies a policy for determining a mode of operation of said first computer entity in relation to said second computer entity.

15. (previously presented) The first computer entity as claimed in claim 11, wherein said network management component operates to:

communicate with a plurality of other computer entities of said network for sending and receiving policy data concerning an operational policy towards said second computer entity; and

determine, from a consideration of policy data received from said other computer entities, a global policy to be adopted by each computer entity in said network, towards said second computer entity.

16. (previously presented) A data storage media comprising:

program data for controlling a first computer entity to perform a method that includes:

operating a peer to peer protocol for enabling said first computer entity to utilise a resource of a second computer entity in a peer to peer network, and for enabling said second computer entity to utilise a resource of said first computer entity in said peer to peer network; and

operating a process, in cooperation with a third computer entity in said peer to peer network, for managing said second computer entity,

wherein said process is automatically invoked whenever said first computer entity takes part in said peer to peer network using said peer to peer protocol.

17. (previously presented) A method performed by a first computer entity, said method comprising:

operating a peer to peer protocol for enabling said first computer entity to utilise a resource of a second computer entity in a peer to peer network, and for enabling said second computer entity to utilise a resource of said first computer entity in said peer to peer network; and managing said second computer entity, in cooperation with a third computer entity in said peer to peer network.

18. (previously presented) The method of claim 1, wherein said process includes considering whether said second computer entity allows said first computer entity to utilise said resource of said second computer entity.

19. (previously presented) The method of claim 5, wherein said determining said network management policy includes considering whether said second computer entity allows said first computer entity to utilise a resource of said second computer entity.

20. (previously presented) The first computer entity of claim 11, wherein said network management component considers whether said second computer entity allows said first computer entity to utilise a resource of said second computer entity.

21. (previously presented) The data storage media of claim 16, wherein said process for managing said second computer entity includes considering whether said second computer entity allows said first computer entity to utilise said resource of said second computer entity.

22. (previously presented) The method of claim 17, wherein said managing considers whether said second computer entity allows said first computer entity to utilise said resource of said second computer entity.

(ix) Evidence Appendix

None.

(x) Related Proceedings Appendix

None.